Please replace the paragraph beginning at page 14, line 21, with the following rewritten paragraph:

--In a case where the decrypted data M, for which copyrights are claimed, is stored in an external device 38, i.e., in a medium such as a digital versatile disk (DVD) RAM or a hard disk, etc., or is transferred externally via a network, the decrypted data M is re-encrypted using the unchangeable key K0 at the encryption unit 36 of the unchangeable key encryption/decryption unit 35:

$$\forall 0: C0 = E(M, K0)$$

$$= E(D(C1, K1), K0),$$

further, the re-encrypted data C0 is double re-encrypted at an encryption unit 40 of the changeable key encryption/decryption unit 39 by using the second changeable key K2:

$$\forall 0\text{-}2: C0\text{-}2 = E(C0, K2)$$

$$= E(E(D(C1, K1), K0), K2),$$

and double re-encrypted data C0-2 is stored in the external device 38 or transferred.--

Please replace the paragraph beginning at page 15, line 11 with the following rewritten paragraph:

-- In a case where the double re-encrypted data C0-2 is used again, the re-encrypted data C0-2 read from the storage medium of the external device 38 or transferred from the

network is re-decrypted using the external changeable key K2 by the re-decryption unit 41 of the external changeable key encryption/decryption unit 39:

$$\exists:0:C0 = [E]\ \underline{D}\ (C0\text{-}2, K2)$$

$$=D\ (E\ (E\ (D\ (C1, K1), K0), K2),$$

further, the re-decrypted data C0 is again re-decrypted using the unchangeable key K0 by a decryption unit 37 of the unchangeable key encryption/decryption unit 35:

$$\exists:M = D\ (C0, K0)$$

$$=D\ (E\ (D\ (C1, K1), K0)$$

and the decrypted data M is outputted to the display unit 34 or the like.--

Please replace the paragraph beginning at page 16, line 5, with the following rewritten paragraph:

--As described above, because the re-encryption is performed using the unchangeable key K0 before the re-encryption using the second changeable key K2, even when the unchangeable key K0 is discovered by others, since the data is also encrypted by using the second changeable key K2, it is very difficult to cryptanalyze the encrypted data without further finding out the second changeable key K2.--

Please replace the paragraph beginning at page 16, line 14, with the following rewritten paragraph:

--In the description of this embodiment, the encryption unit 36 and the decryption unit 37 are contained in the unchangeable key encryption/decryption unit 35 and the encryption unit 40 and the decryption unit 41 are contained in the changeable key encryption/decryption unit 39. Of course, it goes without saying that these units 36, 37, 40 and 41 may also be separately provided.--

Please replace the paragraph beginning at page 20, line 17, with the following rewritten paragraph:

--The operating system 51 comprises an operating system service 52 and a system service API 53, which are user regions, and a kernel 54 and a HAL 55, which are non-user regions. The system service API 53 is arranged between the operating system service 52 and the kernel 54 and serves to mediate between the operating system service 52 and the kernel 54. The HAL 55 is arranged at the lowermost layer of the operating system 51 and serves to absorb differences in the hardware for the software.--

Please replace the paragraph beginning at page 22, line 13, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 is utilized, the double re-encrypted data C2-0 read from the storage medium or transferred via the network is re-decrypted using the unchangeable key K0 at the unchangeable key encryption/decryption unit 57:

∃2:C2 = [E] D (C2-0, K0)

= D (E (E (D (C1, K1), K2), K0).

Further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the HAL 55 having the changeable key encryption/decryption function:

∃:M = D (C2, K2)

= D (E (D (C1, K1), K2),

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.--

Please replace the paragraph beginning at page 25, line 12, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 is utilized again, the double re-encrypted data C2-0 read from the storage medium or transferred via the network is re-decrypted using the unchangeable key K0 at the internal unchangeable key encryption/decryption unit 57:

∃2:C2=D (C2-0, K0)

=D (E (E (D (C1, K1), K2), K0).

Further, the re-decrypted data C2 is decrypted by the filter driver 66A or 66B, using the second changeable key K2:

∃:M = D (C2, K2)

=D (E (D (C1, K1), K2)

and the decrypted data M thus obtained is outputted to the display unit 56 or the like. --

Please replace the paragraph beginning at page 26, line 1, with the following rewritten paragraph:

--The filter driver can be easily placed into the kernel of the operation system in a part of the I/O manager. In so doing, the function of the re-encryption/re-decryption processing and the key management can be easily incorporated into the operation system. Also, since re-encryption is performed using the second changeable key K2 before the re-encryption using the unchangeable key K0, even if the unchangeable key K0 is discovered by others, it is very difficult to cryptanalyze the encrypted data without finding out the second changeable key K2 because the data is also encrypted by the second changeable key K2.--

A9

Please replace the paragraph beginning at page 26, line 8, with the following rewritten paragraph:

--Further, because the second changeable key K2 is used first, and is then, used after the unchangeable key K0 is used, the key security can be highly ensured. Also, because the second changeable key K2 is used first, it strongly governs the encrypted data.--

A10

Please replace the paragraph beginning at page 26, line 13, with the following rewritten paragraph:

--In a fifth embodiment shown in Fig. 7, the changeable key encryption/decryption and the key management is provided by software carried out at the disk driver 67 and the network driver 68 contained in the I/O management micro-kernel 64 in the operating system 51.--

Please replace the paragraph beginning at page 28, line 1, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 is utilized again, the double re-encrypted data C2-0 read from the storage medium or transferred via a network is re-decrypted using the unchangeable key K0 by the internal unchangeable key encryption/decryption unit 57:

$\exists 2: C2 = D(C2\text{-}0, K0)$

$= D(E(E(D(C1, K1), K2), K0).$

Further, the re-decrypted data C2 is decrypted by the device driver 71, i.e., the disk driver 67 and the network driver 68, using the second changeable key K2:

$\exists: M = D(C2, K2)$

$= D(E(D(C1, K1), K2)$

and the decrypted data M thus obtained is outputted to the display unit 56 or the like.--

Please replace the paragraph beginning at page 31, line 14, with the following rewritten paragraph:

--When the re-encrypted data C2-0 stored in the storage medium 81 is utilized, the double re-encrypted data C2-0 read from the storage medium 81 is decrypted using the unchangeable crypt key K0 placed in a decryption unit 17 of the internal unchangeable key encryption/decryption unit 15:

$$\exists 2: C2 = D(C2\text{-}0, K0)$$
$$= D(E(E(D(C1, K1), K2), K0)$$
$$= E(E(D(C1, K1), K2),$$

further, the re-decrypted data C2 is decrypted using the changeable key K2 by a decryption unit 21 of the changeable key encryption/decryption unit 19:

$$\exists: M = D(C2, K2)$$
$$= D(E(D(C1, K1), K2)$$

and the decrypted data M is outputted to the display unit 14 or the like.--

Please replace the paragraph beginning at page 32, line 4, with the following rewritten paragraph:

--In this case, in order to ensure security, when the double re-encrypted data C2-0 is read from the storage medium 81 via a path shown by a broken line in the figure, it may be designed in a manner that the double re-encrypted data C2-0 in the storage medium 81 is erased at that

time, and that the data re-encrypted using the changeable key K2 and the internal unchangeable key K0 is stored again.--

Please replace the paragraph beginning at page 35, line 12, with the following rewritten paragraph:

--In this case, in order to ensure security, when the double re-encrypted data C0-2 is read from the storage medium 81 via a route shown by a broken line in the figure, it may be designed in a manner that the double re-encrypted data C0-2 in the storage medium 81 is erased at that time, and that the data re-encrypted using the second changeable key K2 and the unchangeable key K0 is stored again.--

Please replace the paragraph beginning at page 36, line 8, with the following rewritten paragraph:

--When the double re-encrypted data C3-2 sent to the externals 82 is utilized, the double re-encrypted data C3-2 is decrypted using the second changeable key K2 by the decryption unit 84 of the changeable key encryption/decryption unit 83:

$$\exists 3: C3 = D(C3\text{-}2, K2)$$

$$= D(E(C3, K2), K2),$$

further, the re-encrypted data C3 thus obtained is decrypted using the third changeable key K3 by the decryption unit 85 of the changeable key encryption/decryption unit 83:

A16

$\exists$: M = D (C3, K3)

= D (E (M, K3), K3)

and the decrypted data M thus obtained is outputted to the display unit 86 or the like.--

Please replace the paragraph beginning at page 37, line 17, with the following rewritten paragraph:

A17

--For this purpose, changeable key encryption units 90 and 91 are provided as hardware 88, in addition to the unchangeable key encryption/decryption unit 89. In a case where the copyrighted and decrypted data is stored in the hard disk 81 of the storage medium incorporated in or dedicated to the computer, it is double re-encrypted and decrypted using the unchangeable key K0 by the encryption/decryption unit 89 via a disk driver 67. In a case where the data is stored in the DVD-RAM 92 of the removable medium, it is double re-encrypted and decrypted using the third changeable key K3 by the encryption/decryption unit 90 via the disk driver 67. In a case where the data is transferred externally via the network 93, it is double re-encrypted and decrypted using the third changeable key K3 by the changeable key encryption/decryption unit 91 via a network driver 68.--

Please replace the paragraph beginning at page 39, line 6, with the following rewritten paragraph:

--In a case where the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the double re-encrypted data C2-0 read from the storage medium 81 is re-decrypted using the unchangeable key K0 by the encryption/decryption unit 89 in the hardware 88:

$\exists 2$: C2 = D (C2-0, K0) =D (E (E (D (C1, K1), K2), K0),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the filter driver 66 having encryption/ decryption function:

$\exists$: M=D (C2, K2) =D (E (D (C1, K1), K2),

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.--

Please replace the paragraph beginning at page 39, line 15, with the following rewritten paragraph:

--When the re-encrypted data C2 is stored in a DVD-RAM of the removable medium, the re-encrypted data C2 is double re-encrypted using the third changeable key K3 by the changeable key encryption/decryption unit 90 of the hardware:

$\forall 2\text{-}3$: C2-3=E (C2, K3) =E (E (D (C1, K1), K2), K3)

and double re-encrypted data C2-3 is stored in the removable medium, the DVD-RAM.--

Please replace the paragraph beginning at page 43, line1, with the following rewritten paragraph:

--When the double re-encrypted data C2-0 stored in the storage medium 81 is utilized, the double re-encrypted data C2-0 read from the storage medium 81 is re-decrypted using the unchangeable key K0 by the encryption/decrypted unit 89 in the hardware 88:

$\exists 2$: C2 = D (C2-0, K0) =D (E (E (D (C1, K1), K2), K0),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the filter driver 66 having encryption/decryption function:

$\exists$: M = D (C2, K2) =D (E (D (C1, K1), K2)

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.--

Please replace the paragraph beginning at page 43, line 16, with the following rewritten paragraph:

--When the double re-encrypted data C2-3 stored in the removable medium 92 is utilized, the re-encrypted data C2-3 read from the removable medium 92 is re-decrypted using the third changeable key K3 by the encryption/decryption unit 90 in the hardware 88:

$\exists 2$: C2 = D (C2-3, K3) =D (E (E (D (C1, K1), K2), K3),

further, the re-decrypted data C2 is decrypted using the second changeable key K2 by the filter driver 66 having encryption/decryption function:

$\exists$: M = D (C2, K2) =D (E (D (C1, K1), K2)

A21

and the decrypted data M is outputted by the operating system of the computer to the display unit 56 or the like to be utilized.--

---

Please replace the paragraph beginning at page 47, line 3, with the following rewritten paragraph:

A22

--In Fig. 12, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive 106, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.--

---

Please replace the paragraph beginning at page 47, line 19, with the following rewritten paragraph:

A23

--In cases where the decrypted digital data M is stored in the hard disk drive 105, where it is copied at the flexible disk drive 106 or where it is transferred via the modem 108, the decrypted digital data is re-encrypted using the second changeable key K2 by the encryption unit 112:

$\forall$2: C2 = E (M, K2)

= E (D (C1, K1), K2),

the re-encrypted digital data C2 is supplied to the system-bus 102, and is stored in the hard disk drive 105, copied in the flexible disk drive 106 or transferred via the modem 108.

Please replace the paragraph beginning at page 49, line 7, with the following rewritten paragraph:

--In Fig. 13, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive 106, a CD-ROM drive 107, a modem 108, etc. are connected to a system-bus 102 connected to the CPU 101.--

Please replace the paragraph beginning at page 51, line 8, with the following rewritten paragraph:

--When the decrypted digital data M is stored at the hard disk drive 105 or is copied at the flexible disk drive 106 or is transferred via the modem 108, it is re-encrypted using the second changeable key K2 by the encryption unit 112:

$\forall$=2: C2 = E (M, K2)

= E (D (C1, K1), K2),

the re-encrypted digital data C2 is supplied to the system-bus 102, and it is stored at the hard disk drive 105, copied at the flexible disk drive106, or transferred via the modem 108.--

Please replace the paragraph beginning at page 52, line 5, with the following rewritten paragraph:

--When the encrypted audio signal Ca0 is inputted to the encrypted audio data player 126 from the crypt audio interface 123, it is decrypted using the unchangeable key K0 by the unchangeable key decryption unit 129:

A26

Ma=D (Ca0, K0),

the decrypted audio signal Ma is converted to a playable analog signal by the D/A converter 132, and it is played by the speaker 117.--

Please replace the paragraph beginning at page 53, line 8, with the following rewritten paragraph:

A27

--In Fig. 14, reference numeral 101 represents a CPU. A ROM 103, a RAM 104, a hard disk drive 105, a flexible disk drive 106, a CD-ROM drive 107, a modem 108, etc., are connected to a system-bus 102 connected to the CPU 101.--

Please replace the paragraph beginning at page 53, line 11, with the following rewritten paragraph:

A28

--Reference numeral 140 represents a copyright management apparatus, which comprises a decryption/encryption unit 110, a video interface 113, an audio interface 114, a printer interface 141, and an unchangeable key encryption unit 134.--

Please replace the paragraph beginning at page 53, line 14, with the following rewritten paragraph:

A29

--The decryption/encryption unit 110 has a decryption unit 111 and an re-encryption unit 112.--

Please replace the paragraph beginning at page 53, line 16, with the following rewritten paragraph:

A30

--The unchangeable key encryption unit 134 has an unchangeable key encryption unit for video 135, an unchangeable key encryption unit for audio 136, and an unchangeable key encryption unit for print 137. The unchangeable key encryption units for video, audio and print may be arranged in a single unit if it is available for sufficient encryption capacity.

Please replace the paragraph beginning at page 53, line 20, with the following rewritten paragraph:

A31

--The decryption unit 111 and the re-encryption unit 112 of the decryption/encryption unit 110 are connected to the system-bus 102 of the computer. Further, the video interface 131, the audio interface 132 and the printer interface 133 are connected to the decryption unit 111, and the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 136 and the unchangeable key encryption unit for print 137 are connected to these interfaces.--

Please replace the paragraph beginning at page 54, line 7, with the following rewritten paragraph:

A32 --The above arrangement can be easily realized by designing the copyright management apparatus 140 as a sub-computer arrangement having a CPU and a system-bus.

Please replace the paragraph beginning at page 55, line 5, with the following rewritten paragraph:

A33 --When the decrypted digital data M is stored at the hard disk drive 105 or copied at the flexible disk drive 106 or transferred via the modem 108, it is re-encrypted using the second changeable key K2 by the encryption unit 112:

$\forall 2$: C2=E (M, K2)

=E (D (C1, K1), K2),

the re-encrypted digital data C2 is supplied to the system-bus 102, and it is then stored at the hard disk drive 105, copied at the flexible disk drive 106 or transferred via the modem 108.

Please replace the paragraph beginning at page 55, line 12, with the following rewritten paragraph:

A34 --When the decrypted digital data M is outputted to the encrypted data display unit 125, the encrypted audio data player 126 or the encrypted data printer 127, the decrypted digital data M is arranged to digital data Md, Ma and Mp to be provided to the display unit 116, the speaker

117 and the printer 118 respectively at the video interface 131, the audio interface 132 and the printer interface 133 in the copyright management apparatus 140. Then, these digital data are encrypted using the unchangeable key K0 by the unchangeable key encryption unit for video 135, the unchangeable key encryption unit for audio 136 and the unchangeable key encryption unit for print 137:

A34

Cd0=E (Md, K0)

Ca0=E (Ma, K0)

Cp0=E (Mp, K0)

and the encrypted display signal Cd0, the encrypted audio signal Ca0 and the encrypted print signal Cp0 are outputted.--

Please replace the paragraph beginning at page 56, line 17, with the following rewritten paragraph:

--The encrypted print signal Cp0 is inputted to the encrypted data printer 127 from the unchangeable key encryption unit 137, and it is decrypted using the unchangeable key K0:

A35

Mp=D (Cp0, K0).

The decrypted print signal Mp is printed by the printer 118..--